MSc in Photonics

PHOTONICS**BCN**

Universitat Politècnica de Catalunya (UPC)
Universitat Autònoma de Barcelona (UAB)
Universitat de Barcelona (UB)
Institut de Ciències Fotòniques (ICFO)

http://www.photonicsbcn.eu

Master in Photonics

MASTER THESIS WORK

COHERENCE-BASED QUANTUM RANDOM NUMBER GENERATOR

Juan Rafael Álvarez Velásquez

Supervised by Prof. Juan P. Torres (ICFO, UPC)

Presented on date 27th August, 2018

Registered at

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

Coherence-based quantum random number generator

JUAN RAFAEL ÁLVAREZ VELÁSQUEZ,[1,2,3,*]

[1] *ICFO-Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[2] *Universitat Politècnica de Catalunya (UPC)–Barcelona Tech, 08034 Barcelona, Spain*
[3] *Aix Marseille Université, CNRS, Centrale Marseille, Institut Fresnel, UMR 7249, 13013 Marseille, France*
[*] *Juan-Rafael.Alvarez@icfo.eu*

Abstract:
We consider the random change of the phase of a laser as the physical source of randomness that allows the implementation a new type of quantum random number generator (QRNG) . We analyze the phase noise model of a laser and study how randomness can be extracted with the help of optical coherent detection. We also demonstrate an ultra-fast QRNG of up to 19 Gbits/s of random numbers that use commercial devices already found in the laboratory.

This master's thesis was written under the supervision of Prof. Dr. Juan P. Torres, and the experiments were carried out in the Optical Communications Laboratory in the Universitat Politècnica de Catalunya. It is presented to opt for the title of Master in Photonics, Europhotonics.

1. Introduction

In this master thesis we make use of coherence detection to implement two complementary approaches for implementing a QNGR. We implement two different experimental set ups that examine particular quantum phenomena that are inherently random and thus we are able to study and characterize fast random phenomena that could be used for industrial applications. We have implemented QRNG with a speed beyond a few Gigabits per second, that is considered nowadays ultrafast. During the development of this thesis, the main sections describe:

1. The conditions necessary for random number generation using a Continuous Wave (CW) Laser, by calculating the probability distributions arising from accessing the phase of a laser in a Mach-Zehnder Interferometer (MZI) powered by such a laser, as initially conceived and tested by Hoi-Kwong Lo *et al.* [1].

2. Some of the reasons for the convenience on using an optical hybrid to enhance the random number generation speed. We discuss some of the different signal processing techniques used for this enhancement, as well as for the obtention of random strings.

3. A variant of the originally proposed experiment, amplifying the fluctuations of the electromagnetic vacuum according to a previous proposal [2], which promises to generate secure key rates up to 19Gbps.

4. The callibration of a randomness extractor and the measurement different statistical testing suites (Diehard, NIST, TestU01) on the strings of random data measured from our experiments.

1.1. Why random number generators?

Random numbers are routinely needed and used in many branches of science and technology, among which we can count statistical analysis, computer simulation and cryptography [1, 3]. Random numbers are present everywhere in many of our daily activities: banking, commerce,

gambling. In communications they constitute a basic element of the so-called key distribution problem, a basic element of secure communications, classical and quantum. In science, they are behind powerful simulation methods such as Montercarlo.

There is a large amount of Random Number Generators (RNGs) implemented in the computing systems that we use. Most of these generators use algorithms which by definition have a determined periodicity [3]. This poses a security threat for the use of random numbers, especially when the generation rates required are extremely high. Because of this, algorithmically programmed RNGs are called Pseudorandom number generators, or PRNGs.

On sharp contrast with algorithmic RNGs, Physical Random Number Generators have no underlying periodicity and they collect their randomness based on the measurement of a physical phenomenon that is intrinsically random. In fact, modern computer operating systems use physical random number generators that are able to collect randomness from the environment of a computer: the keystrokes, temperature variations and other physical phenomena are used to extract randomness from the environment by physical mechanisms [3]. In fact, many public organisms and even countries are creating their own random number generators using phenomena such as earthquakes, cryptocurrencies, radio streams, or even tweets [4].

Unlike classical random phenomena, which is based on the lack of knowledge on deterministic variables, randomness in Quantum Mechanics arises intrinsically from the very foundations of the field. Due to this, there is a wide variety of methods and mechanisms that can generate random numbers using quantum phenomena. In fact, the first Quantum Random Number Generator ever implemented was based in the decay of radioactive nuclei [3].

Light has interesting features that allowed the scientific community to envision optically based QRNGs: its speed, the ease in the detection and the maturity of optical technologies have allowed optically based QRNGs to become the largest category of QRNGs.

Many methods are built based on the use of single photon sources, which rely on meticulous experimental techniques that lower the rate of random numbers which can be generated. Due to this, many of the modern techniques for ultra-fast QRNGs rely on macroscopic measurements of variables which can exhibit quantum randomness behind them. Three of the most used methods are phase noise, electromagnetic vacuum fluctuations and amplified spontaneous emission, among other different methods [3]. In fact, this master's thesis aims to show how a coherent detector, a device used in quantum optics for sensitive measurements and in telecommunications for high capacity transmission schemes, can be used in random number generation to exploit the connection between phase noise and electromagnetic vacuum fluctuations.

2. How to generate random sequences

As mentioned before, a physical random number generator, whatever physical phenomenon it lies on, has an intrinsic amount of randomness which is either given by a lack of physical information necessary to reproduce the phenomenon, or a knowledge of a physical process with a non-realizable precision and a heavy dependence on the initial conditions, such as in chaotic systems, or by the intrinsic randomness of Quantum Mechanics. The random physical phenomenon will be known as randomness source or entropy source.

After a randomness source has been identified, the successive measurements of the random phenomenon are recorded digitally with an Analog to Digital Converter (ADC). From the statistics, a probability mass function is obtained, albeit it might not be uniform. Since Random

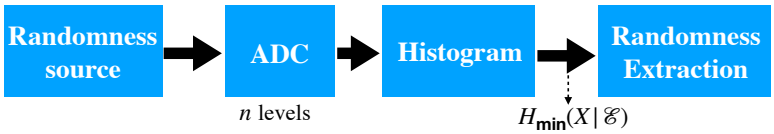

Figure 1. Flow diagram for a Random Number Generator. Randomness is obtained from a physical source, then it is digitalized by an Analog to Digital converter, then a probability mass function is set and from this source a randomness extractor can be used.

Number Generators are expected to be uncorrelated and describe a uniform distribution, a procedure called Randomness Extraction is used. On this basis, a very important quantity for the use of random number generators [2, 5] is the min-entropy of the random data obtained, which is defined as

$$H_{\min}(X) = -\log_2 \max_x P(X = x), \tag{1}$$

where $P(X = x)$ is the probability that the random variable X, obtained from the randomness source, is equal to each of its possible outcomes x. If the probability distribution of the measured random variable is fully trusted, *i.e.*, if we have full control of the external variables that control the randomness source, the min-entropy is interpreted as the quantity of true random bits per sample that can be extracted from the original, raw sample.

If there is a security threat (or even a suspicion) to the randomness of the sample, for example, an eavesdropper controlling the randomness measured, it is necessary to consider a conditional min-entropy bound, this is, an amount of extractable bits which are both secure and random. This quantity, denoted as $H_{\min}(X|\mathcal{E})$, is assessed individually depending on the physical situation that generates the random numbers. As it will be seen in section 4.3, one of our randomness experiments can be bounded to extract secure random numbers.

3. Physical randomness mechanisms

In the next sections, two methods for generating random numbers which can exploit the potential of a coherent detector will be described: measuring the phase noise diffusion of a laser and measuring the fluctuations of electromagnetic vacuum.

3.1. Phase diffusion model for a laser

One possible physical mechanism from which it is possible to obtain randomness is the phase noise of a laser, as it will be introduced here. The phase noise of a laser occurs due to the spontaneous emission events occurring in the laser cavity [6].

Since the spontaneous emission events occurring in the cavity have a random phase, the phase of the total laser diffuses gradually with a certain diffusion equation [6]. It is assumed that spontaneous emission takes place in shorter time scales than the evolution of the field. With a laser operating above threshold, amplitude fluctuations will be ignored.

The positive-frequency electric field component of a laser, $\mathbf{E}^{(+)}(t)$[1], can be written as

$$\mathbf{E}^{(+)}(t) = \sqrt{\langle n \rangle} \exp(i\theta(t) - i\nu_0 t), \tag{2}$$

[1]The total electric field will be a sum of its positive and negative electric field components, *i.e.*, $\mathbf{E}^{(+)}(t) + \mathbf{E}^{(-)}(t) = \mathbf{E}^{(+)}(t) + \text{h.c.}$

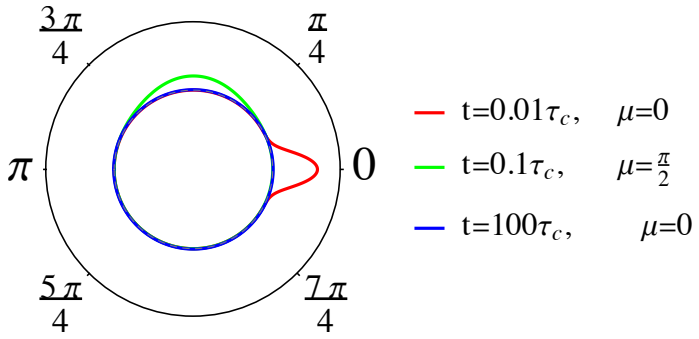

Figure 2. Normal distribution with different values of μ, the mean value of the distribution, after certain scales of the coherence time defined in have passed. We can see that as t, the elapsed time between successive samples, becomes large, the distribution becomes uniform in the angular variable.

where $\langle n \rangle$ is the mean number of photons of frequency ν_0 in the field in steady state and $\theta(t)$ is the angular displacement of the phase, which is random due to the spontaneous emission events occurring in the laser cavity, with a rate equal to $\mathscr{A}$.

Since the amplitude fluctuations are ignored, $\theta(t)$ will describe a one-dimensional real variable, describing a random walk along the unit circle. Indeed, the probability density function (PDF) of $\theta(t)$ is given by a normal distribution:

$$P(\theta, \mu; t) = \sqrt{\frac{\langle n \rangle}{\pi \mathscr{A} t}} e^{-\left((\theta-\mu)^2 \langle n \rangle / \mathscr{A} t\right)}, \tag{3}$$

which satisfies a diffusion equation with a drift coefficient $D = \frac{\mathscr{A}}{4\langle n \rangle}$. Here μ is considered to be the origin of the random walk, the point where the phase starts its random walk when we start measuring. As t becomes larger, the distribution becomes flatter 2 and starts crossing to the other side of the unit circle, thus making a uniform distribution on the unit circle.

With the expression given for the field, the second-order correlation function for the laser is

$$g^{(2)}(\tau) = \left\langle E^{(-)}(t) E^{(+)}(t+\tau) \right\rangle = \langle n \rangle e^{-i\nu_0 t} e^{-D\tau} \sim \exp(-\tau/\tau_c), \tag{4}$$

where $\tau_c = 1/D$ is the coherence time of the source, *i.e.*, the time in which we can assume that the phase of a laser source remains stable. By taking the Fourier transform of $g^{(2)}(\tau)$, we obtain the power spectrum of the laser, which is a Lorentzian distribution centered at $\nu = \nu_0$ with a full width at half−maximum linewidth of $\Delta\nu = 2D = \frac{\mathscr{A}}{2\langle n \rangle}$:

$$S(\nu) = \frac{\langle n \rangle}{\pi} \frac{D}{(\nu - \nu_0)^2 + D^2} \tag{5}$$

Therefore, it is possible to relate the linewidth of the laser with its coherence time: $\tau_c = \frac{2}{\Delta\nu}$.

From this result, we see that the frequency linewidth of a laser will be inversely proportional to its coherence time, thus making wide, lowly coherent lasers preferrable for phase-noise random number generation, as they yield faster key rates. As a matter of fact, the tunable lasers used

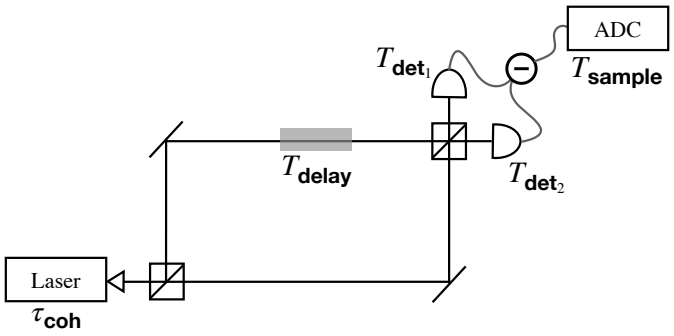

Figure 3. Mach-Zehnder Interferometer introduced for a coherence-based RNG. A laser with a coherence time τ_c is introduced in a Mach-Zehnder interferometer with a balanced detector that subtracts the optical currents coming into detectors D_1 and D_2 with detection times T_{D_1} and T_{D_2}. One of the arms passes through a time delay T_{delay}. The Analog to Digital Converter after the signal subtraction has an integration time T_S.

in the experiments have linewidths in frequency $\Delta\nu \approx 100$kHz, thus having coherence times of $\tau_c \approx 20\mu$s, *i.e.* periods of 20μs where the phase is approximately constant.

By reassigning terms in Eq. 3, we conclude that the variance of the normal distribution is given by $\sigma_P^2 = 2t/\tau_c$. The evolution of the distribution of the phase with respect to the elapsed time between successive measurements is shown in Fig. 2. The phases will diffuse in time, transitioning from a heavily peaked Gaussian when $t \ll \tau_c$, to a uniform distribution when $t > \tau_c/2$, as it can be seen in Figure 2.

4. Accessing to the phase noise of a continuous wave laser

In 2009, Hoi-Kwong Lo *et. al* [1] proposed an experimental setup that uses a laser passing through a Mach-Zehnder Interferometer (Fig. 3) to generate random numbers. This experimental setup is based in the balanced detection of two photocurrents from the same laser that are delayed in time from each other by a time delay T_{delay}.

The power incident on each arm of the interferometer is given by

$$P_{D_1} = P_0 \cos^2\left(\frac{\Delta\phi}{2}\right), \qquad P_{D_2} = P_0 \sin^2\left(\frac{\Delta\phi}{2}\right). \tag{6}$$

Here, $P_0 = \int |E_0|^2\, dt$ is the time integration of the electric field intensity. Since this measurement takes an integration time which is dependent on the detector's response time T_{det}, we require the phase to maintain constant while the measurement is being performed. Additionally, $\Delta\phi$ is the phase difference between the two interferometer arms, which is related to the path difference between these two arms [1]: $\Delta\phi = \nu_0 T_{\text{delay}} + \delta\theta\left(t, T_{\text{delay}}\right)$. Additionally, T_{delay} can be quantified as $T_{\text{delay}} = \frac{n\Delta L}{c}$, with n the refractive index of the medium and c the speed of light.

With $\delta\theta = \theta(t) - \theta\left(t + T_{\text{delay}}\right)$ being the variation in the phase noise of the laser, the balanced detector yields a current that is proportional to

$$\Delta P = P_{D_1} - P_{D_2} = P_0 \cos(\Delta\phi) = P_0 \cos\left(\nu_0 T_{\text{delay}} + \delta\theta\right) \tag{7}$$

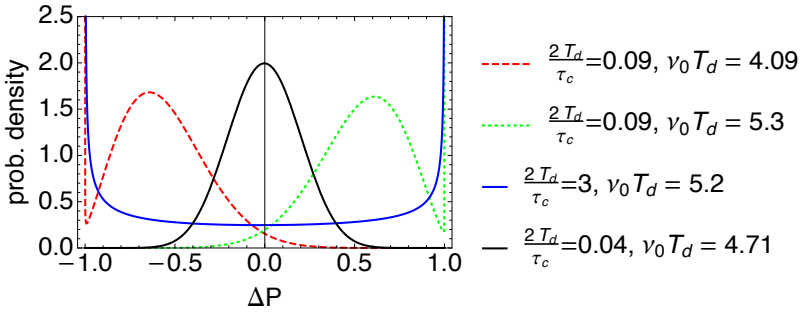

Figure 4. Change of the distribution as T_{delay} and τ_c are tuned. Notice that T_{delay} can be tuned to convert the distribution from a peaked Gaussian to an extremal arcsine. Notice as well that a symmetric Gaussian with zero mean can be achieved. This is the method used by Hoi-Kwong Lo *et al.* [1] to overcome the time delay condition imposed by Eq. 10.

Because of what has been discussed in subsection 3.1, we know that the variance in the distribution of the values for θ is given by $\Delta\theta^2 = 2t/\tau_c$, in such a way that

$$\left\langle \left[\delta\theta\left(t, T_{\text{delay}}\right)\right]^2 \right\rangle = \frac{2T_{\text{delay}}}{\tau_c} \tag{8}$$

Here, $\nu_0 T_{\text{delay}}$ is a real constant, while $\delta\theta$ is a normally distributed random variable with mean 0 and variance $2T_{\text{delay}}/\tau_c$. We want to find the probability density function of ΔP. With this interferometer setup, the quantity that we can sample is ΔP, and because of this we need to know how the probability distribution of ΔP changes with T_{delay}, the time difference between both interferometer arms.

In particular, we want to digitize the differential signal ΔP to obtain random numbers. We would like to have a probability distribution for the digitized signal that is equally likely to have positive and negative values of ΔP. Since T_{delay} changes the variance of a normal distribution, this calculation reduces to obtaining the probability density function of the cosine of a normally distributed random variable. In particular, we would like to know for which values of T_{delay} and ν_0 our distribution is completely symmetric, as this guarantees that we will have a distribution that can generate equal amounts of zeroes and ones. By following the method of obtaining the cumulative distribution of the function and then deriving [7] we find that

$$f_{\Delta P}(p) = \frac{1}{\sqrt{1-p^2}}\left[f_{\delta\theta}\left(2\pi - \cos^{-1}(p) - \nu_0 T_{\text{delay}}\right) + f_{\delta\theta}\left(\cos^{-1}(p) - \nu_0 T_{\text{delay}}\right)\right] \tag{9}$$

where $f_{\delta\theta}(\theta) = P\left(\theta; 0, T_{\text{delay}}\right)$, as in eq. 3.

In Fig. 4 it is possible to see that when $T_{\text{delay}} \gg \tau_c/2$, the distribution becomes more and more similar to the arcsine distribution, which has been widely used for Random Number Generation. This distribution is symmetric and peaked around $\Delta P = \pm 1$. As the time delay between both interferometer arms grows, the distribution will tend to the arcsine distribution that arises when calculating the density function of the cosine of a uniform random variable, which is symmetric.

4.0.1. Conditions for random number generation:

Apart from the already mentioned conditions for time delay and coherence time, other conditions must be satisfied in order to generate random numbers with the proposed Mach-Zehnder

interferometer. If we define the sampling period T_{sample} of the Analog to Digital Converter (ADC) as the reciprocal of the sampling bandwidth, we can summarize the recommended conditions [1] for random number generation as:

1. $T_{\text{delay}} \gg \tau_{\text{coh}}$: We require that the delay is longer than the coherence times to measure uncorrelated phases in both interferometer arms.

2. $T_{\text{sample}} > T_{\text{det}} + T_{\text{delay}} > \tau_{\text{coh}}$: so that samples are taken apart in time from each other, after both detection and Mach-Zehnder delay occur. Since condition 1 already establishes the delay to be longer than the coherence times, we conclude that the sampling times must also be longer than the coherence times.

3. $T_{\text{det}} < \tau_{\text{coh}}$. This implies that, upon integration, the detection time is smaller than the coherence time to make sure that the source shows a perfectly defined constant phase during the time it is being measured.

The last two conditions boil down to one inequality:

$$T_{\text{det}} < \tau_{\text{coh}} < T_{\text{sample}} \tag{10}$$

In the practical implementation to generate randomness using the phase noise of a laser, the condition set in Eq. 10 limits strongly the key rate that can be achieved to the coherence time: Having the coherence time set between two quantities which might be close to each other strongly limits the conditions that an interferometer can meet, and further delays would have to be used.

However, there exists a method to relax the condition 1 imposed by Eq. 10: stabilizing the phase difference between both lasers, $T_{\text{delay}} = n\Delta L/c$, by changing the value of the refractive index on the interferometer by introducing a phase modulator which controls that the distribution of ΔP of the distribution is kept symmetric during the measurements. This makes time delays on the interferometer independent on the measurement of coherence times.

With detectors of around 1GHz of bandwidth and narrowband lasers of 100KHz of linewidth, the random number generation rate achieved cannot exceed the key generation of 100kbits/s: The coherence time of the source is the most important quantity used to generate random keys.

4.1. Interference with two lasers

After having observed and characterized a single-laser system, we investigate on how the use of two lasers can help us achieve faster key rates. We also investigate on the distributions that arise from this situation. More specifically, we want to examine which limiting conditions still hold when we use two lasers in a Mach-Zehnder interferometer setup.

We obtained this idea from the regime of spatial distribution: In the spatial domain there have been observations of interference fringes between two separate pulsed lasers [8]. Louradour *et al.* [8] showed the interference fringes of two separate lasers in two different shots: The two shots are displaced between each other, as if a relative phase between the beams changes in time. The interferometer used by Louradour *et al.* is a Michelson interferometer. However, the sources used here have coherence times which are much larger than the length of the pulses. By switching to the temporal regime, *i.e.*, using a Mach-Zehnder interferometer, it is expected to obtain results in which the random phase changes can be tracked.

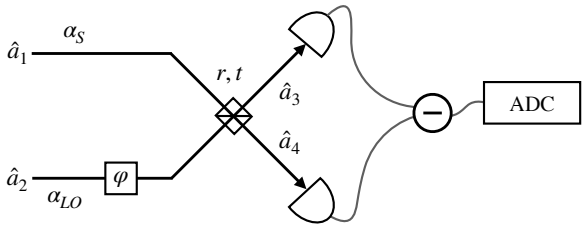

Figure 5. Balanced detector scheme for homodyne detection. Input coherent states $|\alpha_S\rangle$ and $|\alpha_{LO}\rangle$, with creation and annihilation operators $\hat{a}_1$ and $\hat{a}_2$, get converted by the beam splitter with transmittivity t and reflectivity r into creation and annihilation operators $\hat{a}_3$ and $\hat{a}_3$. A phase φ is set in the entry of one of the inputs. The balanced detection measured is $\langle \hat{N}_3 - \hat{N}_4 \rangle$, where $\hat{N}$ is the number operator in the detector.

4.1.1. Balanced detection

The usage of two lasers leads to a treatment of the interferometer as a balanced detector with two inputting coherent states. The use of one balanced detector and two lasers sets a configuration which is known as a homodyne detection if the two lasers have the same frequency, and which has been commonly used for diverse optical measurements. In fact, homodyne detection is a key scheme for Random Number Generation [9, 10]. It also allows the measurement of precise quantities such as gravitational waves, which is the reason why homodyne detection is used in large interferometers such as LIGO [11].

The inputs of the balanced detector are called Signal and Local Oscillator, respectively. The balanced detector allows to measure one quadrature of one of the fields, *i.e.*, either the real or the imaginary part of the complex amplitude of the electric field vector of one of the inputs.

By setting an initial phase in one of the fields of φ, and with electric fields inputting a beam splitter with a reflection coefficient r and a transmission coefficient t which satisfy $|r|^2 + |t|^2 = 1$, it is possible to obtain the following input $(\hat{a}_1, \hat{a}_2)$-output $(\hat{a}_3, \hat{a}_4)$ relation between the creation and annihilation operators of the field:

$$\hat{a}_3 = r\hat{a}_1 + te^{i\varphi}\hat{a}_2, \tag{11}$$

$$\hat{a}_4 = re^{i\varphi}\hat{a}_2 + t\hat{a}_1. \tag{12}$$

By inputting coherent states in the signal ($|\alpha_S\rangle$) and local oscillator ($|\alpha_{LO}\rangle$) inputs, the phase of the Signal input can be estimated by measuring the statistics of the operators S_R and S_I, which depend on the values of r and t. By setting $r = \frac{1}{\sqrt{2}}$ and $t = \frac{-1}{\sqrt{2}}$ the mean value of the signal with $\varphi = 0$, $\langle \hat{S}_R \rangle$ is obtained, and by setting $\varphi = \pi/2$, the mean value of the signal $\langle \hat{S}_I \rangle$ is obtained:

$$\langle S_R \rangle = 2\,|\alpha_{\mathrm{S}}|\,|\alpha_{\mathrm{LO}}|\cos(\theta_{\mathrm{S}} - \theta_{\mathrm{LO}}), \tag{13}$$

$$\langle S_I \rangle = 2\,|\alpha_{\mathrm{S}}|\,|\alpha_{\mathrm{LO}}|\sin(\theta_{\mathrm{S}} - \theta_{\mathrm{LO}}), \tag{14}$$

where $|\alpha_S|^2$ is the mean number of photons of the coherent state of the Signal input, $|\alpha_{LO}|^2$ is the mean number of photons of the coherent state of the Local Oscillator input, θ_S is the phase of the signal input and θ_{LO} is the phase of the LO input. The variance of both values of the signal is equal, and given by

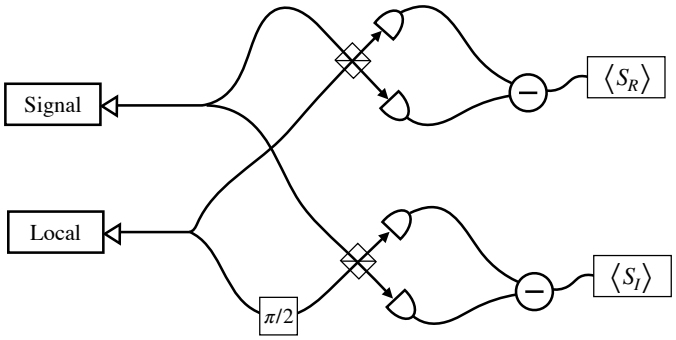

Figure 6. Two-input two-output balanced detector scheme for heterodyne detection. A Signal and a Local Oscillator coherent states are input into two simultaneous homodyne detection schemes, to measure $\langle S_R \rangle$ and $\langle S_I \rangle$ and thus estimate the quadratures of the signal state.

$$\Delta S_{\mathrm{R}} = \Delta S_{\mathrm{I}} = |\alpha_{\mathrm{S}}|^2 + |\alpha_{\mathrm{LO}}|^2 . \tag{15}$$

By tuning the values of the power in the Signal and the Local Oscillator inputs, it is possible to find different means and variances going out from the coherent detector. With $|\alpha_{\mathrm{LO}}|^2 \gg |\alpha_{\mathrm{S}}|^2$, driving $|\alpha_{\mathrm{S}}|^2 \to 0$ will not change the variance significantly but the mean will change significantly.

4.2. Coherent detection

It is possible to implement two simultaneous homodyne detectors such as the ones presented in the previous section. This setting is called a coherent detector (or alternatively, an optical hybrid), and it allows to perform a double-homodyne measurement, this is, the simultaneous measurement of both quadratures of the signal field[2]. A scheme of a coherent detector is shown in Fig. 6. Contrary to physical intuition, the simultaneous measurement of both quadratures of a field is indeed possible in Quantum Mechanics at the expense of gaining more noise in the measurement, as it has been discussed in [12–14].

4.2.1. Phase estimation with a coherent detector

The phase of the signal input can be estimated by using the simultaneous values of $\langle S_{\mathrm{R}} \rangle$ and $\langle S_{\mathrm{I}} \rangle$, by setting $\phi = \arctan \frac{\langle S_R \rangle}{\langle S_I \rangle}$. It is thus possible to calculate the noise of ϕ by using error propagation:

$$(\Delta\phi)^2 = \left(\frac{\partial\phi}{\partial \langle S_R \rangle}\right)^2 (\Delta S_R)^2 + \left(\frac{\partial\phi}{\partial \langle S_I \rangle}\right)^2 (\Delta S_I)^2 = \frac{\left(|\alpha_{\mathrm{S}}|^2 + |\alpha_{\mathrm{LO}}|^2\right)}{4\,|\alpha_{\mathrm{S}}|^2\,|\alpha_{\mathrm{LO}}|^2} \tag{16}$$

If $|\alpha_{\mathrm{S}}|$ is kept constant, we can calculate the variance in the phase measurement:

$$\lim_{|\alpha_{\mathrm{LO}}|\to\infty} \Delta\phi = \frac{1}{2\,|\alpha_S|} = \frac{1}{\sqrt{2N_S}}. \tag{17}$$

[2]In the quantum literature, the double-homodyne measurement is sometimes known as a heterodyne measurement [2].

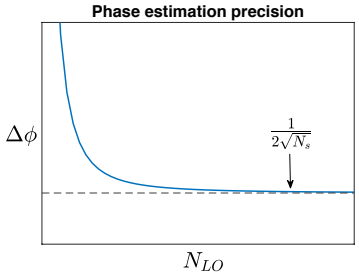

Figure 7. Phase estimation precision $\Delta\phi$ vs. LO power.

We find that the variance of ϕ is in agreement with the shot noise limit [15]. This implies that an infinite power in the local oscillator still yields noise in the measurement of ϕ. However, decreasing $|\alpha_S| \to 0$, the signal input approaches to the vacuum state, which does not have a defined phase. Thus, it is found that

$$\lim_{|\alpha_S|\to 0} \Delta\phi \to \infty. \tag{18}$$

and therefore it is not possible to resolve any phase on a vacuum state. A depiction of these precision limitations is shown in Figure 7. The next section will be devoted to the techniques used to generate random numbers using a vacuum state as signal input.

4.3. Measuring vacuum fluctuations with a coherent detector

Measuring the vacuum fluctuations has been one of the methods used and published for generating random numbers that has had most repercussion [3, 9, 10], but their use had been exclusively limted to homodyne detection until this year (2018). A paper from the group of Paolo Villoresi in Padova showed the use of a heterodyne-based, or phase diversity, random number generator using the vacuum fluctuations [2].

It is possible to think about this setting of Random Number Generation as a communications problem: Alice reads random numbers from a quantum source, which might be controlled a priori by some eavesdropper, Eve. This is what is known in Random Number Generation as a source-device-independent (SDI) random Number Generator: an eavesdropper might be controlling the source and even have prior information on the string of generated random numbers.

By measuring simultaneously both quadratures, it is possible to obtain an exceeded generation rate by doubling the amount of random bits that can be used for the generation of secure keys. The coherent detection measurements can be described with the formalism of Positive Operator Valued Measurements, or POVMs. In the present case, the POVMs make the set $\left\{\hat{\Pi}_\alpha\right\}_{\alpha\in\mathbb{C}}$, where $\hat{\Pi}_\alpha = \frac{1}{\pi}|\alpha\rangle\langle\alpha|$, *i.e.*, the projectors onto the coherent states $|\alpha\rangle$ with amplitudes α.

The output of the heterodyne measurements performed by the coherent detector will be distributed according to the random variable $X = \{\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)\}$, which will follow statistics determined by the following probability density function, called the Husimi function:

$$Q_{\hat{\rho}_A}(\alpha) = \mathrm{tr}\left[\hat{\Pi}_\alpha \hat{\rho}_A\right] = \frac{1}{\pi}\langle\alpha|\,\hat{\rho}_A\,|\alpha\rangle, \tag{19}$$

Where $\hat{\rho}_A$ is the density matrix of the electromagnetic field that Alice will read. This value is expected to follow a Gaussian two-dimensional distribution [2, 16] with variances equal to $1/2$

and zero covariances.

By using the properties of discretized POVMs, Avesani *et al.* [2] derived a lower bound on $H_{\min}(X|\mathcal{E})$ which allows them to calculate, in a real life implementation, $H_{\min}(X|\mathcal{E})$:

$$H_{\min}(X|\mathcal{E}) \geq \log_2 \frac{\pi}{\delta_R \delta_I}, \tag{20}$$

where the measurement in the quadratures R, a measurement of $\langle S_R \rangle$ and I, a measurement of $\langle S_I \rangle$, are discretized in steps δ_R and δ_I, respectively. A practical implementation of this is shown in subsection 5.7.

Therefore, in a physical implementation such as the one shown in [2], the min-entropy required for the estimation of the randomness extraction is dependent only on the measurement resolution, a quantity that comes from the calibration of our detectors and which is kept constant throughout the measurement.

5. Experimental realization

5.1. Two-laser setup

The experimental development of this master's thesis was performed in the Optical Communications Laboratory from the Universitat Politècnica de Catalunya. The used input lasers were tunable laser sources, in particular, the Agilent 8164A and the Hewlett-Packard 8168A, which have tunable wavelengths centered around 1550 nm that can be changed with a resolution so low as 10^{-4}nm. A physical depiction of both lasers can be seen in Fig. 8 (a) . One of the features of these laser sources is their narrow linewidth $\Delta\nu$, which is about 200kHz in each of the sources.

The output of these lasers was sent to an optical hybrid device which can be used for measuring two simultaneous polarizations in a communications QPSK (Quadrature Phase Shift Keying) scheme. The output of such optical hybrid is connected to four balanced detectors PDB480C-AC, as we can see in Fig. 8. The photodetectors yield as outputs the components $\langle S_R \rangle$ and $\langle S_I \rangle$ for both the x and y polarizations of light. These components reveal the phase difference of the lasers used:

$$\langle S_R \rangle \propto \cos\left(2\pi\Delta_f t + \delta\theta\right) \qquad \langle S_I \rangle \propto \sin\left(2\pi\Delta_f t + \delta\theta\right) \tag{21}$$

where P_{sig} and P_{LO} are the optical powers of the signal and local oscillators, $2\pi\Delta_f := \nu_{\text{sig}} - \nu_{\text{LO}}$ is the beating frequency of the system[3], and $\delta\theta = \theta_{\text{sig}}(t) - \theta_{\text{LO}}(t)$ is a random variable constant with the minimum coherence time of the setup.

The $\langle S_R \rangle$ and $\langle S_I \rangle$ components are measured with photodiodes that have bandwidths of 1.6GHz (*i.e.*, a response time of 625 ps). This allows the tracking of changes on the phases much faster than the changes of the phase, thus getting access to the continuous dynamics of the phase difference between the signal and the local oscillator.

With the phase-diversity detection scheme, measuring two quadratures at the same time, it is possible to duplicate the amount of bits that are recorded by the ADC, and thus we can obtain faster key rates than a simpler in-phase or in-quadrature detector could for analogous random number generation.

[3]Thus realizing a heterodyne measurement, since the frequency difference between both lasers can't be tuned to exactly zero

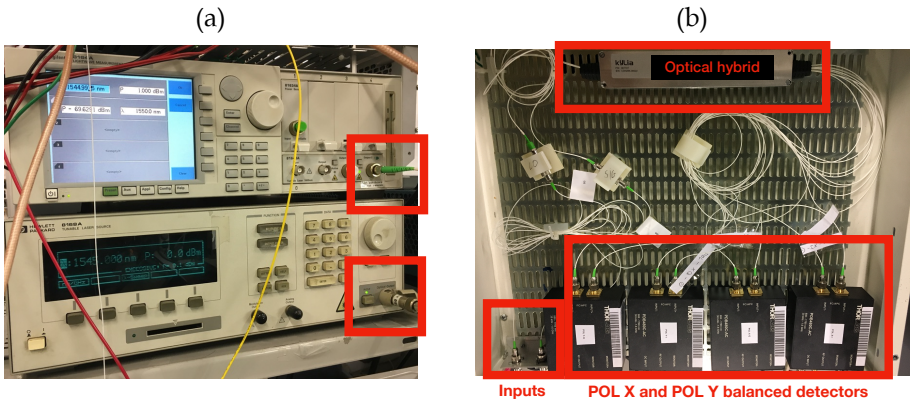

Figure 8. (a) Tunable laser sources, as seen in the Laboratory Implementation. The outputs are shown inside the red boxes. (b) Optical hybrid description. In red boxes, labeled, the inputs, the optical hybrid configuration, and the balanced detectors for both polarizations are seen.

5.2. Retrieving the phase noise from the signal

The randomness in a laser can come from different origins: whether it is fluctuations from current, instabilities of the laser, or drifts in the cavity due to the tunability of the laser, all of these variations might affect the behavior of the laser and its noise. However, most of the external non-quantum noise might be due to deterministic, classical and possibly eavesdropped noise. However, these instabilities end up embedded in the frequency term, and because of this we intend to isolate the random term $\delta\theta$ from any possibly deterministic terms from equation 21.

5.2.1. Unwrapping

We have established that $\delta\theta$ is a noisy term that rides on top of a more stable, linear term of the form $2\pi\Delta_f t$. Given the two quadratures, on any given moment, we can obtain a phase term from our signals

$$\varphi(t) = \text{angle}\left(\langle S_R\rangle + i\,\langle S_I\rangle\right) = 2\pi\Delta_f t + \delta\theta(t)\,. \tag{22}$$

However, the recovery of the value of $\theta(t)$ exhibits discontinuities due to the fact that the range of the function angle lies between $-\pi$ and π. For this reason, we end up having sharp jumps in the phase, something which is not desirable for the processing. This can be seen in Fig. 9.

When facing this problem, one used processing method is called unwrapping [17], which recovers the continuity of the angle by making the curve of $\theta(t)$ a linear function. It is thus possible to convert a curve in radians to a more continuous function which can still yield the same results when displayed in a circular figure. The tolerance of the unwrapping algorithm is adjustable but, by default, when the algorithm finds jumps larger than π it will reconnect the figure to create a continuous function by eliminating the jumps. Thus, upon removing the trendline of the linear term $2\pi\Delta_f t$, it is possible to recover the dynamics of $\delta\theta$.

5.2.2. Cosine shifted spectrum

We can also recover the phase noise of our signal laser by removing the beat term using the cosine shifted spectrum of our signal. Upon identifying the driving frequency (Δ_f) of $\langle S_R\rangle$ and

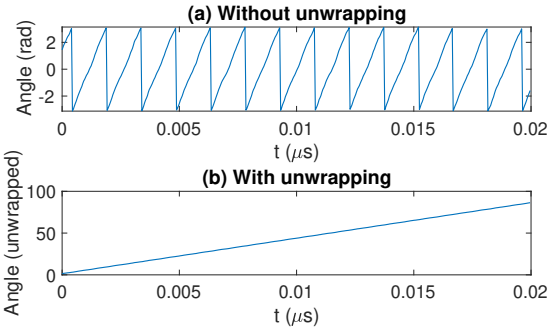

Figure 9. (a) Wrapped phase, calculated as angle $(\langle S_R \rangle + i \langle S_I \rangle)$, recovered from experimental data. The sharp discontinuities constitute an artifact for the processing of the signal. (b) Unwrapped phase. A linear term of the form $2\pi\Delta_f t$ is directly extractable from the unwrapping of the angle.

$\langle S_I \rangle$, we can isolate $\delta\theta$ as follows:

$$\langle S_R \rangle \cos\left(2\pi\Delta_f t\right) + \langle S_I \rangle \sin\left(2\pi\Delta_f t\right) = \cos\left(\delta\theta\right) \tag{23}$$

$$\langle S_I \rangle \cos\left(2\pi\Delta_f t\right) - \langle S_R \rangle \sin\left(2\pi\Delta_f t\right) = \sin\left(\delta\theta\right) \tag{24}$$

Since Δ_f varies in time, the adjustment for obtaining $\delta\theta$ drifts from the actual value. This can be corrected by implementing an algorithm of phase-locked-loop (PLL) to track the variations of Δ_f over the whole range of changes of the signal. Practically, this is equivalent to cutting the signal into k equal slices and performing the treatment shown in Eqs. 23 and 24. It is important to keep a balance between the amount of cuts (in which Δ_f is kept constant) and the number of points in every cut.

With this method, we can follow the time variations of the phase in time for fast sampling rates of 25GSamples/s. For a sample of 20 million points at this sample rate, each point is taken every 40 picoseconds, for a total duration of 0.8 miliseconds. For a laser linewidth of 100KHz, we have coherence times of 10μs, which allow for approximately 80 uncorrelated phases in the whole measurement. We show a graph of the recovered phase, which describes a random walk in the angle, as it can be seen in Figure 10.

5.3. Obtaining the phase diffusion correlation dynamics

As mentioned before, we have noticed that the most important figure to examine here is the value $\delta\theta$, which varies independently from $2\pi\Delta_f$ and can be extracted by using different processing methods.

We have indeed studied that the phase differences obey a diffusion process, having in mind that the initial phase is defined as zero. With different sampling rates and by using the processing methods described before, we can obtain the dynamics of the phase as we take successively separated intervals. This leads to a *wool ball* trajectories, which can be interpreted as a Gaussian distribution in the phase which widens as we take points which are more and more uncorrelated between each other. Fig. 11 describes graphically this situation. This indicates that the trajectories become less correlated as we let the phase diffuse itself, in time orders which correspond to the coherence times described, *i.e.*, $(100\text{kHz})^{-1}$.

We will proceed to describe another way of obtaining random numbers before we test and callibrate our results using a randomness extractor. The combination of randomness extraction

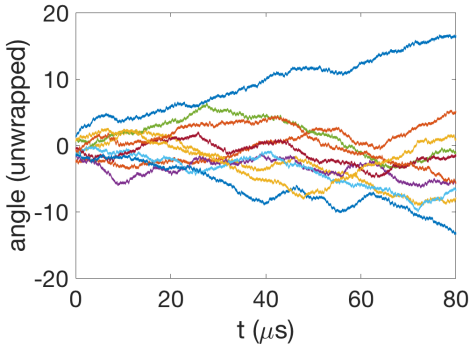

Figure 10. Experimentally recovered temporal evolution of the phase noise for different times of the signal, recovered after performing the cosine shifted spectrum processing method and unwrapping the angle.

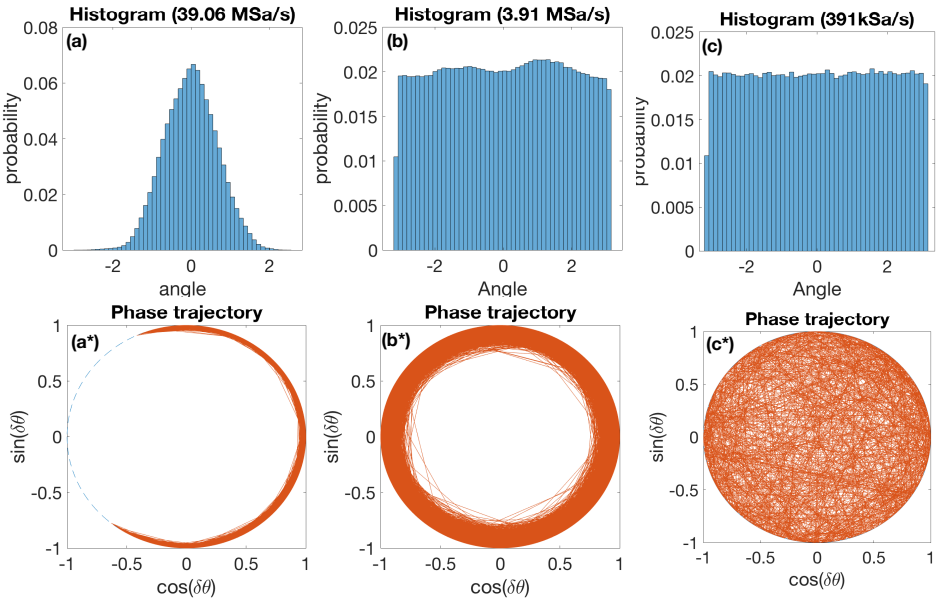

Figure 11. Histogram and phase space representation for three different sample rates: 39.06 MSamples/s, 3.91 MSamples/s, and 391 kSamples/s. The values of the phase transition from a continuous motion in the top figure, describing carefully a trajectory that does not exit from the circle, to a trajectory where every point of the phase is uncorrelated with its previous value. Here the orange line is used to connect successive points, to indicate that the trajectory, which occurs essentially in the phase space, is able to cross the whole circle between neighboring phases.

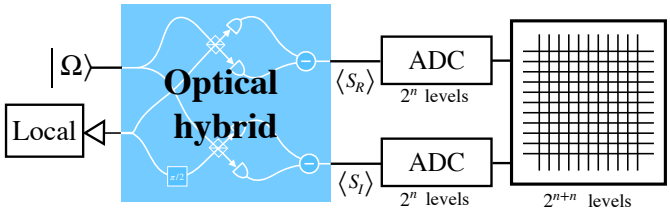

Figure 12. Experimental setup for the single laser random number generator.

and testing will allow us to assess whether our method is correctly measuring the quantum phenomena described in the previous sections.

After having assessed whether the behavior of the phase noise was indeed random for the correct sampling times, we concluded that a random key could be generated by measuring a sample of 24 bits of data (12 for $\langle S_R \rangle$ and 12 for $\langle S_I \rangle$) at 400kSamples/s.

5.4. Single-laser setup

Unlike the two-laser setup, which is based on the measurement of phase noise, the single-laser setup is used to amplify randomness from the vacuum fluctuations, an experimental scheme that has been examined thoroughly for homodyne detection in [3], [9] and [10], and more recently this year in heterodyne/coherent detectors by [2]. The only practical difference between this setup and the previous one is that only one of the lasers is on. For this case, we decided to change the laser for a DFB Laser, (JDS Uniphase CQF935). In this method, the measurement yields a sampling of the vacuum state fluctuations, as we have seen in subsection 4.3. The coherent detector outputs will be directly proportional to the values of the quadratures:

$$V_{D_1} \propto \langle S_R \rangle = \mathrm{Re}\,[\alpha]\,, \qquad V_{D_2} \propto \langle S_I \rangle = \mathrm{Im}\,[\alpha]\,. \tag{25}$$

The values of the voltages are sufficient to recover the shape of the Husimi function of the vacuum state, which, as mentioned before, is a two-dimensional Gaussian distribution with variances equal to $1/2$ [16], but the proportionality constant to be determined will play an important role on the determination of the secure generation rate, as we have seen that the resolution of the quadratures is a key factor in the determination of $H_{\min}\,(X|\mathcal{E})$.

5.5. Bandwidth filtering

One of the questions that arises when seeing the experimental setup shown in Fig. 12 is to know whether the heterodyne detector is indeed amplifying randomness from a vacuum state or just amplifying randomness from the environment, which results in a thermal state.

For guaranteeing the measurement of a vacuum state, it is necessary to limit high and low frequencies in the spectrum of the detector, as background noise can be either thought as a low frequency term, which is almost constant throughout the measurement, or as high-frequency spurious photons. The underlying assumption is that the incoming photons arrive at rates which make them distinguishable from noise, up to some extent.

Because of this, a bandpass filtering of the signal modifies the bandwidth of the detection system, limited by the detector bandwidth of 1.6GHz, and leaves a final bandwidth window of 1.35GHz [2] spanning [0.1GHz, 1.45GHz] .

5.6. Detector calibration

The procedure of detector calibration was done after discussion with Marco Avesani, but a similar procedure is explained by Laudenbach *et al.* [18] in a review paper about Continuous Variable Quantum Key Distribution.

In order to calculate the min-entropy bound for the key generation rate, we must perform a calibration of the detectors. The basic idea is to perform a linear regression on the voltage variance versus the power of the local oscillator [2]. The variance in volts is connected to the variance in quadrature units (also called shot-noise units or natural units) by the power of the Local Oscillator, P_{LO} and a proportionality constant k to be determined [2, 18]: $\sigma_V^2 = kP_{\mathrm{LO}}\sigma_{\langle S\rangle}^2$.

By increasing the power of the local oscillator P_{LO} in the coherent detector and registering the variances in Volts, we get a linear relation: $\sigma_V^2 = mP_{\mathrm{LO}} + c$. In an ideal condition without noise, $c = 0$. However, this never happens in an experimental real-life situation. By convention, in natural units we assume that the vacuum state has a variance of $1/2$, thus $k = 2m$. For an input vacuum state $|\Omega\rangle$ and a given value of P_{LO}, the variances measured by the coherent detector in natural units are given by

$$\sigma_{\langle S\rangle}^2 = \frac{\sigma_V^2}{kP_{LO}} = \frac{mP_{LO} + c}{2mP_{LO}} = \frac{1}{2} + \frac{c}{2mP_{LO}} \tag{26}$$

This value is always larger than $\frac{1}{2}$ for $c \neq 0$. Because of this, the sampled variances of the Husimi function are always larger than the variance of the vacuum state, reducing the value of securely extractable randomness.

With a power on the Local Oscillator $P_{LO} = 3.9\mathrm{mW}$, we calculate that $k_{\langle S_R\rangle} = 28.93\mathrm{mV}^2/\mathrm{NU}$, while $k_{\langle S_I\rangle} = 26.43\mathrm{mV}^2/\mathrm{NU}$. To obtain our values in Natural Units, we will divide our voltages by $\sqrt{k_{\langle S_R\rangle/\langle S_I\rangle}P_{LO}}$ to obtain values in shot noise units. From this result, we obtain a 3d histogram which samples the Husimi function of the prepared vacuum state, as seen in Figure 13 (b).

5.7. Secure generation rate

The bit-precision given by the oscilloscope (or for a $j-$bit digitizer) [10] of our values, in voltages, is $\delta_j = \frac{p_{\max}}{2^{j-1}}$, where $p_{\max}$ is the maximum value of the oscilloscope in its scale setting. In our case, $p_{max} = 250\mathrm{mV}$, and thus with $j = 12$ we have that

$$\delta_{I,V} = \delta_{Q,V} = \frac{250\mathrm{mV}}{2^{11}} = 0.122\mathrm{mV}. \tag{27}$$

Now, with the presented values of δ_R and δ_I, we have that

$$\delta_{R,\mathrm{NU}} = \frac{0.122\mathrm{mV}}{\sqrt{k_{\langle S_R\rangle}P_{LO}}} = 11.49\times10^{-3}\mathrm{NU}, \qquad \delta_{I,\mathrm{NU}} = \frac{0.122\mathrm{mV}}{\sqrt{k_{\langle S_I\rangle}P_{LO}}} = 12.01\times10^{-3}\mathrm{NU}. \tag{28}$$

Therefore, and as we have mentioned in subsection 4.3, it is possible to establish the minimum bound for secure-bit generation rate as

$$H_{\min}(X|\mathcal{E}) \geq \log_2\left(\frac{\pi}{\delta_{Q,\mathrm{NU}}\delta_{I,\mathrm{NU}}}\right) \approx 14.50 \text{ bits}. \tag{29}$$

Since every measurement contains 24 initial bits (12 for $\langle S_R\rangle$ and 12 for $\langle S_I\rangle$), we now know how to hash our data when it faces a randomness extractor: We reduce the function on a $14.50/24 \approx 60\%$ rate. This means that from every 10 input bits, we will recover 6 uniform

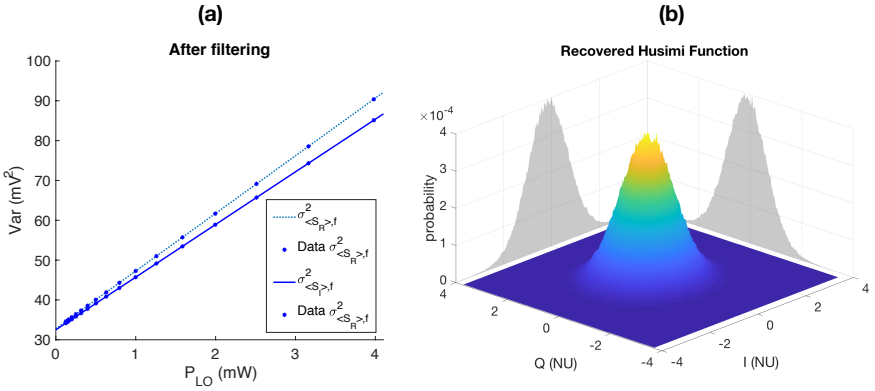

Figure 13. (a) Regression and calibration of the coherent detectors after performing the filter mentioned in subsection 5.5. The linear equations satisfied by the variance will be : $\sigma^2_{\langle S_R \rangle} = 14.5\left(\mathrm{mV}^2/\mathrm{mW}\right) P_{\mathrm{LO}}\,(\mathrm{mW}) + 32.8\left(\mathrm{mV}^2\right)$, whereas $\sigma^2_{\langle S_I \rangle} = 13.2\left(\mathrm{mV}^2/\mathrm{mW}\right) P_{\mathrm{LO}}\,(\mathrm{mW}) + 32.5\left(\mathrm{mV}^2\right)$. (b) Experimentally recovered Husimi function histogram in Natural Units after filtering. The variances obtained are $\sigma^2_R \approx 0.82$ and $\sigma^2_I \approx 0.86$.

output bits sampled from the Gaussian distribution in Fig. 13. With all the security considerations, this method acquires a generation rate which is equal to the secure extractable bits times the filtering window 1.35GHz wide. This gives an equivalent secure generation rate of $\mathcal{R} = 1.35\mathrm{GHz} \times 14.50\mathrm{bits} = 19.6\mathrm{Gbit/s}$.

This is a proof of concept of a Random Number Generator performed with available laboratory components found in an optical laboratory that could reach speeds on the order of Gbps, making it very appealing for its industrial development.

5.8. *Randomness extraction*

Randomness extraction is a procedure that is performed to convert a sequence of discrete, randomly distributed bits following a certain probability mass function, into a uniform distribution. For this, we can use procedures such as two-universal hashing [2, 5, 20] and Trevisan extractors. In two-universal Hashing, the procedure used in this work, we take chunks of the raw vector and hash them (slice them in smaller pieces) by multiplying it by a pseudorandomly generated[4], non-square Toeplitz matrix[5]. Because of the Leftover Hash Lemma [19], the cut output of the raw vector will be uniformly distributed. A practical implementation of a randomness extractor using two-universal hashing is given by Frauchiger *et al.* [20].

In our case, we implemented randomness extractors for both the double and single-laser RNG methods. In the double laser, our hashing was short, as the output looked fairly random in the histograms, much like in Figure 12 (c). Because of this, the Toeplitz matrix used for the hashing had a size of 1024×960, thus obtaining 15 of every 16 bits entered before extraction.

In the case of the vacuum state fluctuations a bound is clear for the extraction of secure numbers. From every 24 bits of extracted data, 14.5 are securely random. The randomness extraction used

[4]This can be paradoxical, as random number generators need random seeds on themselves to be generated and extracted. However, it would be possible to use non-extracted random generated numbers to amplify a seed of randomness.

[5]A Toeplitz matrix is a matrix in which the elements of all its principal and secondary diagonals are constant.

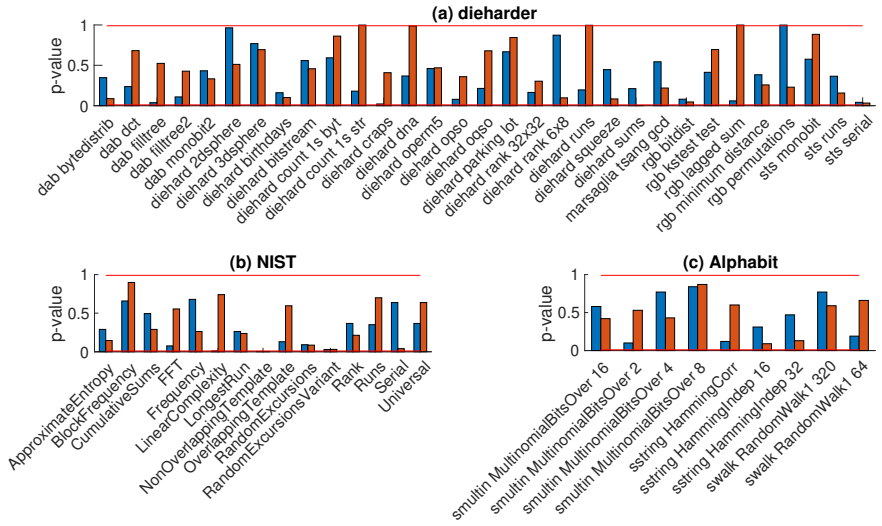

Figure 14. Dieharder, NIST and Alphabit statistical testing suite results. Tests above 0.99 and under 0.01 p-values, indicated on red lines here, are considered weak or failed. Tests in blue (left) correspond to the single-laser approach, i.e., vacuum state fluctuations, and in orange (right) correspond to phase noise. On dieharder, only one test on the vacuum fluctuations and five on the phase noise had a p-value on the weak range, out of all the sets of weak values. On the NIST tests, one of the many overlappingTemplate tests, the only one that fails to appear on this range for both tests, can be interpreted from the results as lacking statistics, as the p-value is around 0.03%. On Alphabit tests, specifically designed for hardware RNG, all tests are passed.

in this case used a 1024×576 Toeplitz matrix, obtaining 9 out of every 16 bits before extraction.

5.9. Randomness Testing

After having recorded the random data from our measurements and correctly verified that the randomness extraction flattens the probability distributions, we would like to test the randomness of the samples generated. For this purpose, we have used three statistical suites generated for the verification of Random Number Generators: Robert G. Brown's **dieharder** [21], US's National Institute of Standards and Technology (NIST)'s Statistical Testing Suite [22], and Pierre L'Ecuyer's TestU01's Alphabit [23].

Randomness tests are based in a statistics concept called hypothesis testing. Hypothesis testing allows us to verify if it is likely that a given sample of population has a certain characteristic that wants to be tested in a general population [24]. In our case, such property is the randomness of our data: We will obtain a $p-$value, the result of a test statistic, that validates the likelihood of our hypothesis. If the sample **PASSES** the test, then $p \in (\alpha, 1-\alpha)$ and the random sample is likely to be random. If the sample is **WEAK**, then $p \in (0, \alpha) \cup (1-\alpha, 1)$ and further evaluation is needed for a decision to be taken, and, if the sample **FAILS** then $p = 0$ or $p = 1$ and the sample is unlikely to be random under the given hypothesis.

For every quadrature we have collected 12 bits of data, accounting for 24 total bits on every sample. This corresponds to 3 bytes for every measurement, saved in a binary file. In Figure 14 we can see the results of the three statistical tests for 18.1 GBytes of data from the single laser

setup and 12.5 GBytes of data from the double laser setup. Among about 250 tests employed (some tests may be repeated various times by the testing suites), the test suites found only a single WEAK test in the single laser setup and no FAILs, and six WEAK tests in the double laser setup. Whenever a test was repeated, we presented its smallest or weakest p-value. Thus, even though the phase noise two-laser approach only failed five tests, all of them are reported in Figure 14. The use of statistical testing suites do not imply that the samples are random *per se*, but it allow us to identify potential failures in the design of RNGs.

6. Conclusions and perspectives

1. After characterizing the randomness for phase noise and vacuum fluctuation methods, we have found that the fastest and, by now, most *random* method, is the vacuum fluctuations method. This is due to the fact that less elements are used for generating faster keys of up to 19Gbps with a lower amount of processing needed. However, both the single and double laser methods employ the same tools and thus they are complementary rather than opposing: The tools for characterizing the optical hybrid and for manipulating the lasers are almost identical, and their calculations were similar in many ways.

2. The methods presented here are on the verge of the state of the art in Quantum Random Number Generation techniques, using methods that are under preparation for publishing. One of the key features of these two methods is the availability of the elements used, and the fact that they can profit from elements which are already commonly used in optical communications laboratories.

3. The availability of most of the optical components needed for these random number generation methods makes their mass-production easy, due to the readily available optical elements. We have estimated a price for all of the components of about 10000 euros (1000 laser, 4000 balanced detectors, 2000 hybrid, 3000 analog to digital converter), therefore we could develop a prototype to produce 100 times the amount of random data of an IDQuantique product at only three times the price offered (1.6Gbps at 10000 euros vs. 16Mbps at 2990 euros [25]).

4. We were able to understand the different processing techniques which are relevant for measuring the phase noise of the laser using a different technique than the ones reported in other works [26] by using a coherent detector.

5. Following equation 5.7, we were able to identify the two critical variables used for enhancing the speed of a Random Number Generator using a coherent detector. We tried to use detectors having a wider bandwidth (FINISAR BPDV2120R, 43GHz bandwidth), but the output of these was so low that no power of Local Oscillator was able to perform a detector callibration. With the appropriate measurement devices, this could be the door to a Random Number Generator exceeding key rates of 100GBits/s, which is extremely competitive in the current state of the art of Random Number Generators.

6. A connection with the other method that can use Coherent Detectors for RNG, Amplified Spontaneous Emission, is called for. It would be interesting to try new ideas over a method that is fast and robust for the generation of random keys.

Acknowledgments

In the technical aspects, I want to thank professor Juan P. Torres, who was the scientific mentor of this project and knew what kind of physics we wanted to learn from it, professors José A. Lázaro and Joan M. Gené, who kindly helped me with the laboratory setting of my thesis, and Samael Sarmiento, whose help in the laboratory has been invaluable for the results that are presented here. I also thank Marco Avesani for helping me with the callibration of the detectors, and Santiago Zubieta for the implementation of the randomness extractor. I also thank professor Morgan Mitchell for the useful discussions. On the personal aspects, I would like to thank my mother for her unconditional support during all of these years, Jorge Madrid and Lluc Sendra for being amazing friends who were always there for me, Veronica Vicuña for listening to my reflections and technical doubts, professor Alejandra Valencia for being a mentor and role model as a scientist, Fundació Catalunya-La Pedrera's ICFO Summer Fellows program for hosting me in the last couple of months, and the Europhotonics POESII master for making this dream true.

References

1. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Optics Letters 35, 312 (2010).
2. M. Avesani, D. G. Marangon, G. Vallone and P. Villoresi, "Secure heterodyne-based quantum random number generator at 17 Gbps" - arXiv:1801.04139.
3. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. 89, (2017).
4. S. Chen, "Why are countries creating public random number generators?," Science (2018).
5. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A 87, (2013).
6. M. O. Scully and M. S. Zubairy, Quantum Optics (Cambridge University Press, 1997).
7. Gabriel's answer, found in Mathoverflow's forum: https://goo.gl/JX4o3N.
8. F. Louradour, F. Reynaud, B. Colombeau, and C. Froehly, "Interference fringes between two separate lasers," Am. J. Phys. 61, 242–245 (1993).
9. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics 4, 711 (2010).
10. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-Device-Independent Ultrafast Quantum Random Number Generation," Phys. Rev. Lett. 118, (2017).
11. P. Fritschel, M. Evans, and V. Frolov, "Balanced homodyne readout for quantum limited gravitational wave detectors," Opt. Express 22, 4224 (2014).
12. K. Kikuchi, "Fundamentals of Coherent Optical Fiber Communications," J. Lightwave Technology 34, 157–179 (2016).
13. E. Arthurs and J. L. Kelly, "On the Simultaneous Measurement of a Pair of Conjugate Observables," Bell System Technical Journal 44, 725–729 (1965).
14. Y. Yamamoto and H. A. Haus, "Preparation, measurement and information capacity of optical quantum states," Rev. Mod Phys. 58, 1001–1020 (1986).
15. R. Paschotta, article on 'shot noise' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3.
16. A. Furusawa, Quantum States of Light, Springer-Briefs in Mathematical Physics No. Volume 10 (Springer, 2015).
17. M. Gdeisat and F. Lilley, "One-Dimensional Phase Unwrapping Problem". https://goo.gl/RqZ6ep.
18. F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations," Adv. Quant. Tech 1800011 (2018). - 10.1002/qute.201800011.
19. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," IEEE Trans. on Inf. Theory 57, 5524–5535 (2011).
20. D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices" arXiv:1311.4547v1.
21. R. G. Brown, D. Eddelbuettel, and D. Bauer, "Dieharder: A Random Number Test Suite. Version 3.31.1," https://webhome.phy.duke.edu/~rgb/General/dieharder.php.
22. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo - "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" - https://goo.gl/MXJQoZ.
23. P. L'Ecuyer and R. Simard, TestU01: A C Library for Empirical Testing of Random Number Generators, ACM Trans. on Math. Software, Vol. 33, 4, article 22, 2007
24. E. L. Lehmann and J. P. Romano, Testing Statistical Hypotheses, 3. ed, Springer Texts in Statistics (Springer, 2005).
25. "Quantis QRNG - Online shop," IDQuantique https://www.idquantique.com/shop/online-shop/.
26. C. Henry, "Theory of the linewidth of semiconductor lasers," IEEE J. Qu. Electronics 18, 259–264 (1982).